NODE, METHOD AND COMPUTER READABLE MEDIUM FOR OPTIMIZING PERFORMANCE OF SIGNATURE RULE MATCHING IN A NETWORK

ABSTRACT OF THE INVENTION

A node of a network for managing an intrusion protection system, the node comprising a memory module for storing data in machine-readable format for retrieval and execution by a central processing unit and an operating system comprising a network stack comprising a protocol driver and a media access control driver and operable to execute an intrusion protection system management application, the management application operable to receive text-file input from an input device, the text-file defining a network-exploit rule and comprising at least one field is provided. A method of distributing command and security updates in a network having an intrusion protection system comprising generating a text-file defining a network-exploit rule and specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file is provided. A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of reading input from an input device of the computer, compiling the input into a machine-readable signature file comprising machine-readable logic representative of the network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field, evaluating the machine-readable signature file, and determining the value of the at least one field of the machine-readable signature file is provided.